

**NETWORK MONITORING APPLICATION FOR IPV6
NETWORK WITH IPSEC**

MOHAMMAD AASHRAFUL AASHIQUE

**A dissertation submitted in partial fulfillment
of the requirements for the award of the degree
of Master of Engineering
(Electrical-Electronics & Telecommunication)**

**Faculty of Electrical Engineering
University Technology of Malaysia**

April, 2005

"To My Loving wife, My Sweet Daughter Tahsin, My Parents and Sis"

ACKNOWLEDGEMENT

All praises to ALLAH for the guidance and strength given to complete this project.

I would like to express my gratitude to my supervisor Associate Professor Dr. Norsheila Binti Fisal for her kind guidance, advice and valuable suggestion throughout the implementation of this project.

I would like to convey my deepest gratitude to all of my friends (urmi, simi, rimi, punam, razu, mokles, wali, rusha, aymen, asif, abdu, muiz, haider, bd, fahim, sumit, himu, biplob, lucy, zia, rico, jahid, jubaer, munna, sayem, muna). Appreciation is also extend to all people who gave the author heartfelt corporation and shared their knowledge and for giving some of their valuable time.

I would also like to thank my friend Sara, for her unselfish support, great understanding and convincing attention during the hectic periods.

Finally, I would like to send my deep appreciations to my wife, my daughter, my sister and my parents.

ABSTRACT

With the increasing need for fast and reliable network connectivity, there has been an exponential rise in the number of local area networks. The networks are becoming bigger and more complex. To ensure that networks function efficiently, network monitoring and management is needed to detect any malfunctioning and take corrective measures. Network monitoring is also useful for observing network performance and traffic patterns, for planning changes and upgrades.

In this thesis, the network monitoring application having Graphical User Interface (GUI) for IPv6 network that will support IP Security. The Linux Router will check the all IP packets from the network, if IP packets has IPSec bits then its secured otherwise it will discard. The IPSec-Policy-MIB which will be take the filtering log to the database. The GUI will show the filtering log to the monitoring system. The router will intercept packets from network interfaces flowing through it and the monitoring application will display the appropriate information.

ABSTRAK

Dengan keperluan rangkaian penghubung yang semakin meningkat, terdapat pertambahan yang pesat dalam rangkaian kawasan setempat. Kini, rangkaian tersebut telah menjadi semakin besar dan kompleks. Bagi memastikan rangkaian tersebut berfungsi secara lancar, pengurusan dan pemantauan rangkaian diperlukan untuk mengesan sebarang kerosakan dan kemudiannya menjalankan pembaikan yang sepatutnya. Pemantauan rangkaian juga diperlukan untuk memerhati pelaksanaan dan bentuk laluan, serta bagi perancangan perubahan dan meningkatkan keupayaan.

Tesis ini meliputi aplikasi pemantauan rangkaian yang menggunakan Pengguna Antara Muka Grafikal untuk rangkaian IPv6 yang menyokong keselamatan IP. Laluan Linux akan memeriksa semua paket IP daripada rangkaian, jika paket IP tersebut mempunyai bit IPSec yang selamat, atupun ia akan disingkirkan. IPSec-Policy-MIB akan menapis pangkalan data. Pengguna Antara Muka Grafikal akan menunjukkan log penapisan kepada sistem pemantauan. Aplikasi pemantauan akan mempamirkan informasi yang berkaitan dan rangkaian laluan akan memintas paket daripada rangkaian antara muka yang mengalir melaluinya.

TABLE OF CONTENTS

CHAPTER	TITLE	PAGE
	TITLE	i
	DECLARATION	ii
	DEDICATION	iii
	ACKNOWLEDGEMENT	iv
	ABSTRACT	v
	ABSTRA K	vi
	TABLE OF ONTENTS	vii
	GLOSSARY OF TABLES	x
	GLOSSARY OF FIGURES	xi
	LIST OF ABBREVIATION	xiii
	LIST OF APPENDICES	xiv
1	INTRODUCTION	
	1.1 Pre liminary	1
	1.2 Objective	1
	1.3 Scope of work	2
	1.4 Project Outline	2
2	THEORETICAL BACKGROUND	
	2.1Introduction	3
	2.2 Internet Protocol Version 6 (IPv6)	4
	2.2.1 Benefits of IPv6	4
	2.2.2 The IPv6 Address Space	5
	2.2.3 IPv6 Header	6

2.3 Internet Protocol Security (IPSec)	7
2.3.1 IPSec basics)	7
2.3.2 IPSec atchitecture	8
2.3.3 AH and ESP	8
2.4 Simple Network Management Protocol (SNMP)	9
2.4.1 Network management components	10
2.4.2 SNMP Protocol	10
2.4.3 SNMP Message Construct	11
2.4.4 Outline of the SNMP Protocol	11
2.4.5 SNMP operation	12
2.4.6 Security levels with basic SNMP	16
2.5 Managed Information Base	16
2.5.1 Criteria and Philosophy for standardized MIB	17
2.6 Net SNMP	18
2.7 FreeS/WAN IPSec	19

3

CONFIGURATIONS AND IMPLEMENTATION

3.1 Introduction	21
3.2 System Process	21
3.2.1 Configuration of IPv6 Network	22
3.2.1.1 Add an IPv6 address	25
3.2.1.2 Add an IPv6 route through a gateway	26
3.2.1.3 Configuration file for Ethernet	26
3.2.2 Configuration of IPSec	27
3.2.3 Configuration of SNMP	28
3.2.4 IPSec Policy MIB	29
3.2.5 GUI Design and Software Coding	29

4	RESULT AND DISCUSSION	
	4.1 Introduction	30
	4.2 Ethernet Status	30
	4.3 Ping Status	31
	4.4 IPSec Route	35
	4.5 IPSec Showdefault	36
	4.6 IPv6 Route	37
	4.7 IPSec Process	38
	4.8 Pluto Log	39
	4.9 Snmp Table	40
	4.10 Final Accepted Log	41
	4.11 Final Discarded Log	42
	4.12 Discussion	43
5	CONCLUSION AND SUMMARY	
	5.1 Summary	44
	5.2 Conclusion	44
	5.3 Recommendation for Future works	45
	REFERENCES	46
	APPENDIX A	49
	APPENDIX B	51
	APPENDIX C	56
	APPENDIX D	63

GLOSSARY OF TABLES

TABLE NO.	TITLE	PAGE
1	IPv6 enabling option in the kernel	24

GLOSSARY OF FIGURES

FIGURE NO.	TITLE	PAGE
0	Network Diagram of the system	4
1	IPv6 header format	6
2	IPSec tunnel and transport mode	7
3	ESP Format	9
4	Management via SNMP	12
5	Structure of management information hierarchy	13
6	Structure of management information through the system group	14
7	MIB object for sysName	15
8	SNMP agent behavior	15
9	MIB	17
10	Final system process	22
11	command ifconfig output	31
12	Ping Status	32
13	Ping Status	32
14	Ping Status	33
15	Ping Status	33
16	Ping Status	34
17	IPSec Route address	35
18	IPSec Showdefaults result	36
19	IPv6 Routing address	37
20	IPSec Process running	38
21	IPSec Pluto Log	39

22	SNMP System Table	40
23	GUI is showing Accepted Logs	41
24	GUI is showing Discarded Logs	42

LIST OF ABBREVIATION

IPv6	Internet Protocol Version 6
IPSec	Internet Protocol Security
SNMP	Simple Network Management Protocol
MIB	Management Information Base
AH	Authentication Header
ESP	Encapsulated Security Payload

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
A	IPSec configuration file	49
B	IPSec start-up script	51
C	Java Code	56
D	IPSec Policy MIB	63

CHAPTER ONE

INTRODUCTION

1.1 Preliminary

Network monitoring is the essential part of the network management. Day by day the network becomes so bigger and more complex. To ensure that networks function efficiently, network monitoring is needed to detect any malfunctioning and take corrective measures. Network monitoring is also useful for observing network performance and traffic patterns, for planning changes and upgrade.

1.2 Objectives

To develop a network monitoring application for IPv6 network that support of IP Security.

1.3 Scope of Research

- Compilation of the kernel “version 2.4.20” which supports IPv6 and IP security has done.
- Configuration of the FreeS/WAN IPSec for the kernel 2.4.20 has successfully achieved.
- Configuration of the Net-SNMP v5.2.1 and IPSEC-POLICY-MIB module has done.
- The tunneling from IPv6 to IPv4 has done successfully.
- The Linux Router has checked all IP packets from the network, if it has IPSec bits then it has been secured otherwise it has been discarded

1.4 Project Outline

The project is organized into five chapters. The outline is as follows:

Chapter 1 -Introduction

A general introduction beside the objectives and scope of this project was stated in this chapter.

Chapter2- Project Overview

In this chapter the theory of IPv6, IPSec, SNMP, MIB, FreeS/WAN IPSec, Net-SNMP were discussed

Chapter3- Configurations and Implementation

This chapter described how the entire configuration for the IPv6 networking, SNMP, IPSec-Policy-MIB, Net-SNMP and FreeS/WAN IPSec was done in the Linux system.

Chapter4- Result and discussion

All the final results were obtained from the system were shown in this chapter.

Chapter5- Conclusion and Summary

The project summary and conclusion was discussed in this chapter.

REFERENCES

- [1] Hui Huang; Jian Ma; Communication Technology Proceedings, 2000. WCC - ICCT 2000. International Conference on , Volume: 2 , 21-25 Aug. 2000, “*IPv6 - future approval networking*”.
- [2] Goode, R.; Military Communications Conference, 1998. MILCOM 98. Proceedings., IEEE , Volume: 1 , 18-21 Oct. 1998, “*Next generation Internet Protocol-testbed experience*”.
- [3] Raicu, I.; Zeadally, S.; Telecommunications, 2003. ICT 2003. 10th International Conference on , Volume: 2 , 23 Feb.-1 March 2003, “*Evaluating IPv4 to IPv6 transition mechanisms*”.
- [4] Lee, D.C.; Lough, D.L.; Midkiff, S.F.; Davis, N.J., IV; Benchoff, P.E.; Network, IEEE , Volume: 12 , Issue: 1 , Jan.-Feb. 1998, “*The next generation of the Internet: aspects of the Internet protocol version 6*”.
- [5] Afifi, H.; Toutain, L.; Computers and Communications, 1999. Proceedings. IEEE International Symposium on , 6-8 July 1999, “*Methods for IPv4-IPv6 transition*”.
- [6] Kanda, M.; Miyazawa, K.; Esaki, H.; Applications and the Internet Workshops, 2004. SAINT 2004 Workshops. 2004 International Symposium on , 26-30 Jan. 2004, “*USAGI IPv6 IPsec development for Linux*”.
- [7] Hagino, J.; Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on , 27-31 Jan. 2003 , “*Implementing IPv6: experiences at KAME project*”.
- [8] Man Li; Network, IEEE , Volume: 17 , Issue: 6 , Nov. -Dec. 2003, “*Policy-based IPsec management*”.

- [9] Chien-Lung Wu; Wu, S.F.; Narayan, R.; Computer Communications and Networks, 2001. Proceedings. Tenth International Conference on , 15-17 Oct. 2001 , “*IPSec/PHIL (packet header information list): design, implementation, and evaluation*”.
- [10] Perlman, R.; Kaufman, C.; Enabling Technologies: Infrastructure for Collaborative Enterprises, 2001. WET ICE 2001. Proceedings. Tenth IEEE International Workshops on , 20-22 June 2001 , “*Analysis of the IPSec key exchange standard*”.
- [11] Keromytis, A.D.; Ioannidis, J.; Smith, J.M.; Global Telecommunications Conference, 1997. GLOBECOM '97., IEEE , Volume: 3 , 3-8 Nov. 1997, “*Implementing IPsec*”.
- [12] Perlman, R.; Kaufman, C.; Internet Computing, IEEE , Volume: 4 , Issue: 6 , Nov.-Dec. 2000, “*Key exchange in IPSec: analysis of IKE*”.
- [13] IPSEC Protocol Overview
www.freesoft.org/CIE/Topics/141.htm
- [14] An IPsec tunnel implementation
http://ringstrom.mine.nu/ipsec_tunnel/
- [15] Intranet Journal – “Understanding IPsec”
http://www.intranetjournal.com/articles/200206/se_06_13_02a.html
- [16] Mitsuru Kanda, Kazunori Miyazawa, iroshi Esaki USAGI IPv6 IPSec Development for Linux
- [17] S. Kent and R. Atkinson. “*IP uthentication Header*”.
RFC2402, November 1998.
- [18] S. Kent and R. Atkinson. “*IP Encapsulating Security Payload*”.
RFC2406, November 1998.
- [19] S. Kent and R. Atkinson. “*Security Architecture for the Internet Protocol*”.
RFC2401, November 1998.
- [20] T. Narten, E. Nordmark, and W. Simpson. “*Neighbor Discovery for IP Version 6 (IPv6)*”. RFC2461 December 1998.
- [21] CryptoAPI Project. <http://www.kernel.org/>.
- [22] FreeSwan project. <http://www.freeswan.org/>.
- [23] Peter Bieringer “*Linux IPv6 HOW TO*”
www.tldp.org/HOWTO/Linux+IPv6-HOWTO/
- [24] elecom Lab – “*IPv6 header format*”

<http://www.ngnet.it/e/ipv6proto/ipv6-proto-1.php>

[25] Net-SNMP. www.net-snmp.org

[26] RFC 3418 – “*MIB for SNMP*”

[27] David T. Perkins and Evan McGinnis, Prentice Hall PTR, 03 December, 1996 ,
“*Understanding SNMP MIBs*“.

[28] H. Erik Hia – Blacksburg Virginia April 23, 2001, “*Secure SNMP-Based
Network Management in Low Bandwidth Networks*”.

[29] P. Martinez, M. Brunner, J. Quittek F. Strauß, J. Schönwälder, S. Mertens, T.
Klie , “*Using the Script MIB for Policy-based Configuration Management*” .